

Via ECFS

February 28, 2011

Marlene H. Dortch
Office of the Secretary
Federal Communication Commission
445 12th Street SW
Suite TW-A325
Washington, DC 20554

Re: **EB DOCKET NO. 06-36**
CERTIFICATION OF CPNI FILING (February 28, 2011)

Dear Ms. Dortch:

Pacific LightNet, Inc. doing business as Wavecom Solutions ("Wavecom Solutions"), hereby files a copy of its 2010 Annual CPNI Compliance Certificate, as required by section 64.2009(e) of the Commission's rules.

Please let me know if you have any questions about this filing.

Sincerely,



Simon Fiddian
Chief Technology Officer


Cc: Best Copy and Printing, Inc. (BCPI), fcc@bcpiweb.com,
Federal Communications Commission, Enforcement Bureau, Telecommunications
Consumers Division, 445 12th Street, SW, Washington, DC 20554

Wavecom Solutions
CPNI COMPLIANCE CERTIFICATE
EB Docket No. 06-36

I, SIMON FIDDIAN, hereby certify as follows:

1. I am the Chief Technology Officer of Wavecom Solutions. In this capacity, I have personal knowledge of Wavecom Solutions' operating procedures concerning customer proprietary network information (CPNI).
2. I provide this certification for the calendar year ending December 31, 2010, in accordance with Commission rule 47 C.F.R. 64.2009(e) (together with such other rules contained at 47 C.F.R. 64.2001, et seq, as the same may be modified, amended or clarified, from time to time, collectively, the "CPNI Rules").
3. The attached Statement of CPNI Compliance explains how Wavecom Solutions operating procedures ensure that it is in compliance with the CPNI Rules.
4. The Company has not taken any actions against data brokers in the past year.
5. The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Certified this 28th day of February, 2011.



SIMON FIDDIAN

ATTACHMENT TO 2009 CPNI COMPLIANCE CERTIFICATE

Statement of CPNI Compliance

I SIMON FIDDIAN sign this Statement of CPNI Compliance in accordance with Section 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and the FCC's Code of Federal Regulations (CFR) Title 47 § 64.2009, on behalf of Pacific LightNet, Inc. doing business as Wavecom Solutions ("Wavecom Solutions"). This Statement addresses the requirement of 47 CFR § 64.2009 that the Company provide both a Certificate of Compliance and a "statement accompanying the certificate" to explain how its operating procedures ensure compliance with 47 CFR § 64.2001-.2009.

On behalf of Wavecom Solutions, I certify as follows:

1. I am the Chief Technology Officer of the Company. My business address is 1132 Bishop Street, Suite 800, Honolulu, Hawaii 96813.
2. I have personal knowledge of the facts stated in this Certificate of Compliance. I am responsible for overseeing compliance with the FCC rules relating to customer proprietary network information (CPNI). The Company qualifies as a "small business concern."
3. The Company conducts ongoing training for its personnel addressing the definition and categories of CPNI, procedures to safeguard CPNI, and procedures to report breaches of CPNI. Personnel who make unauthorized use of CPNI are subject to disciplinary action, up to and including termination.
4. During 2010, Wavecom Solutions did not use, access, or disclose CPNI for the purpose of its sales and marketing campaigns or for services outside the category of services already subscribed to by the customer. In the event Wavecom Solutions authorizes use of CPNI in any future sales and marketing campaigns, the Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company's policy is to maintain these records in its offices for a minimum of one year.
5. Prior to any solicitation for customer approval, the Company will provide notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI in accordance with 47 CFR 64.2008. The Company's policy is to maintain records of customer approval for use of CPNI, as well as notices required by the FCC's regulations, for a minimum of one year, in a readily-available location that can be consulted on an as-needed basis so that the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

6. The Company's policy is to maintain records of a CPNI breach for a minimum of two years. These records will include a description of the steps the Company took to prevent the breach, how the breach occurred, the impact of the breach and proof of notification to law enforcement and the customer, if applicable.
7. During 2010 Wavecom Solutions did not use, access, or disclose CPNI to conduct outbound marketing. The Company has a supervisory review process regarding compliance with the FCC's rules relating to protection of CPNI for outbound marketing situations. The purpose of this supervisory review process is to ensure compliance with all rules prior to using CPNI for a purpose for which customer approval is required. Company personnel, prior to making any use of CPNI, must first consult with me regarding the lawfulness of using the CPNI in the manner contemplated. In deciding whether the contemplated use of the CPNI is proper, I consult with one or more of the following: the Company's own compliance manual, the applicable FCC regulations, the FCC's Compliance Guide, and, if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval from me regarding any proposed use of CPNI.
8. In 2010 Wavecom Solutions experienced two security breaches resulting in unauthorized access to CPNI. As described in the reports filed at the time, Wavecom Solutions addressed each incident as follows:
 - a. On June 23, 2010 a carrier report notified Wavecom Solutions of a spike in its outbound call volume to international countries. Upon investigation, Wavecom Solutions discovered a hacker using a Conficker virus permutation accessed staff credentials and penetrated the company's 808Netfone VoIP system. The engineering team identified and blocked the call routes being used and then identified a source IP Address range initiating additional call attempts and blocked those IPs. We changed the root passwords for all Unix servers and Ser SIP passwords on all accounts used to make unauthorized calls. Passwords for staff accounts with root access were also changed. The virus was removed from all infected devices. Database command logs revealed certain details of unauthorized access to the VoIP system, but logs were not available to determine the complete extent of the breach. Available evidence showed limited access to CPNI data, but it is technically possible that all data in the VoIP database system was compromised and logging information was erased or avoided by the intruder. The following corrective action was taken to mitigate the risk of a similar future security breaches: (i) antivirus and Windows updates were run on all servers and computers; (ii) a security vulnerability fix was applied to manage.808netfone.com; (iii) passwords were changed for the 808Netphone signup websites; (iv) admin.808netfone.com was modified to use LDAP. All unauthorized charges were removed from billing records. On July 2, 2010 the incident was reported to the F.C.C. On July 11, 2010 the F.C.C assigned request ID 2010-1139028, stated that the case had been reviewed, and no action was being taken.

- b. On August 14, 2010 a hacker accessed staff credentials and penetrated the company's 808Netfone VoIP system. Approximately 300 call attempts were made over a short period of time to three international destinations and all but six calls were blocked. Our staff noticed the incident and identified a pattern of unauthorized use for those calls. Upon investigation we identified the call routes being used and blocked them. We changed 808Netfone hardware device session passwords for all 808Netfone customer services. To prevent further intrusions, all credentials were changed, and we locked down all remote systems to internal network access only. Database command logs and system process accounting logs reveal the commands used to access the VoIP account table and call records. These logs indicate that no further data intrusions were made. As corrective action, Wavecom Solutions setup a SSH proxy within the corporate network. All unauthorized charges were removed from billing records. On August 30, 2010 the incident was reported to the F.C.C. On September 8, 2010 the F.C.C assigned request ID 2010-1278841, stated that the case had been reviewed, and no action was being taken.

9. Authentication and data controls include, but are not limited to, the following:

- (i) CPNI "cheat sheet" outlining customer authentication procedures posted at the work stations of all Customer Service Representatives.
- (ii) Hard disk encryption software installed on all Company laptops.
- (iii) Password protection enforcement on all Company issued Blackberry's.
- (iv) Physical security policy to control access to building suites and collocations.
- (v) Usage policy for company computers.
- (vi) Internet policy for controlling information uploaded/downloaded to and from the internet.
- (vii) Password policies.

10. The Company enters into confidentiality agreements, as necessary, with any joint venture partners or independent contractors to whom it discloses or provides access to CPNI.

11. I personally oversee completing and submitting the EB Docket No. 06-36 compliance certificate.



Simon Fiddian
Chief Technology Officer
Wavecom Solutions
February 28, 2011